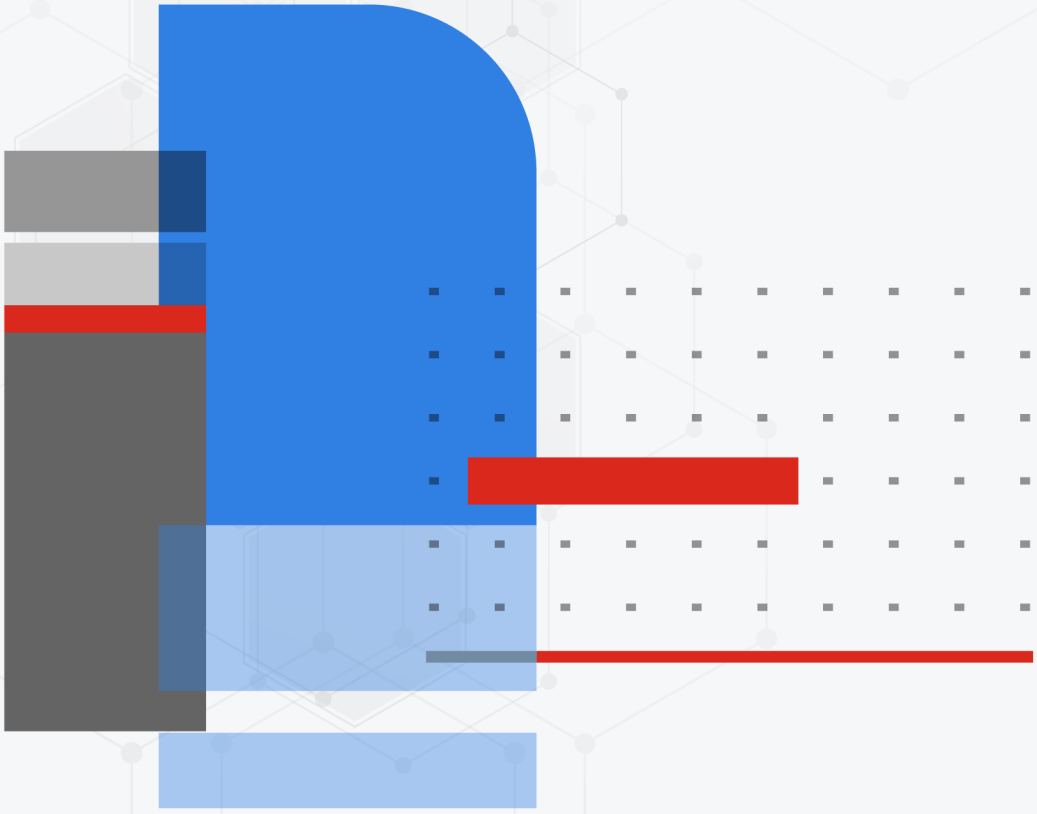
# Release Notes

**FortiNDR 7.4.8**



**FORTINET DOCUMENT LIBRARY**
https://docs.fortinet.com

**FORTINET VIDEO LIBRARY**
https://video.fortinet.com

**FORTINET BLOG**
https://blog.fortinet.com

**CUSTOMER SERVICE & SUPPORT**
https://support.fortinet.com

**FORTINET TRAINING & CERTIFICATION PROGRAM**
https://www.fortinet.com/training-certification

**FORTINET TRAINING INSTITUTE**
https://training.fortinet.com

**FORTIGUARD LABS**
https://www.fortiguard.com

**END USER LICENSE AGREEMENT**
https://www.fortinet.com/doc/legal/EULA.pdf

**FEEDBACK**
Email: techdoc@fortinet.com

April 24, 2025
FortiNDR 7.4.8 Release Notes
55-748-1148463-20250417

# TABLE OF CONTENTS

# Change Log

| Date | Change Description |
| --- | --- |
| 2025-04-22 | Initial release. |
| 2025-05-15 | Updated Resolved issues on page 13. |

# Introduction

FortiNDR (On-premise) is Fortinet's Network Detection and Response product designed for on-premises installations where network metadata remains within the network, supporting OT and air-gapped infrastructure. It is available in various form factors, including appliances, VM/KVM, and public cloud (BYOL), with support for distributed sensors and centers. FortiNDR can classify both network-based and file-based (malware) threats, providing network visibility, including East-West traffic in datacenter/cloud environments. Equipped with Artificial Neural Networks (ANN), it classifies malware into attack scenarios, surfaces outbreak alerts, and traces the source of malware infections. It detects network-based attacks such as intrusions, botnets, compromised IOCs, weak ciphers, and vulnerable protocols. Supervised and unsupervised Machine Learning (ML) continuously analyze metadata across networks to identify threats, with remediation available via Fortinet Security Fabric.

# Licensing

Please refer to the FortiNDR ordering guide for licensing details:
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/og-fortindr.pdf.

Customers must have the correct SKU for FortiNDR functionalities to work.

## Netflow and Scada licenses

Netflow and Scada licenses are ordered separately for sensors and standalone deployment.

# Upgrade information

The latest FortiNDR firmware versions are available for download from FortiCloud. You should always backup your system configuration before upgrading the firmware on your device. Be aware that some configuration settings are not saved to the backup configuration file and will need to be manually restored after upgrade.

## Firmware

FortiNDR 7.4.8 supports the following upgrade path:

| Upgrade from | Upgrade to | Notes |
|---|---|---|
| 7.4.7 | 7.4.8 | |
| 7.4.0 - 7.4.6 | 7.4.7 | Direct upgrade is supported. |
| 7.2.0 - 7.2.4 | 7.4.0 | Direct upgrade is supported. |

- Direct upgrade from v7.0.x, 7.1.x, 7.2.x to v7.4.7 is not supported to v7.4.8 is not supported in any platform.

**Upgrading to major versions:**
You can upgrade from the last minor version to the first new major version. For example, you can upgrade from version 7.2.4 to version 7.4.0.

### FNR-1000F, FNR-3500F (gen3 and above)

- 7.4.8 firmware is designed to run on FNR-1000F and FNR-3500F (gen3 and above) and is not compatible with older FAI-3500F hardware (gen1/2). For more information, see Supported models on page 12.

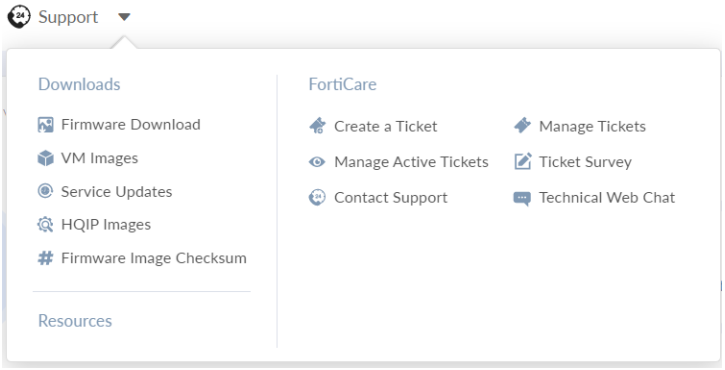
### VM Devices

If your current version FortiNDR does not have a password, you will be prompted to create a password after upgrading, otherwise you cannot login.

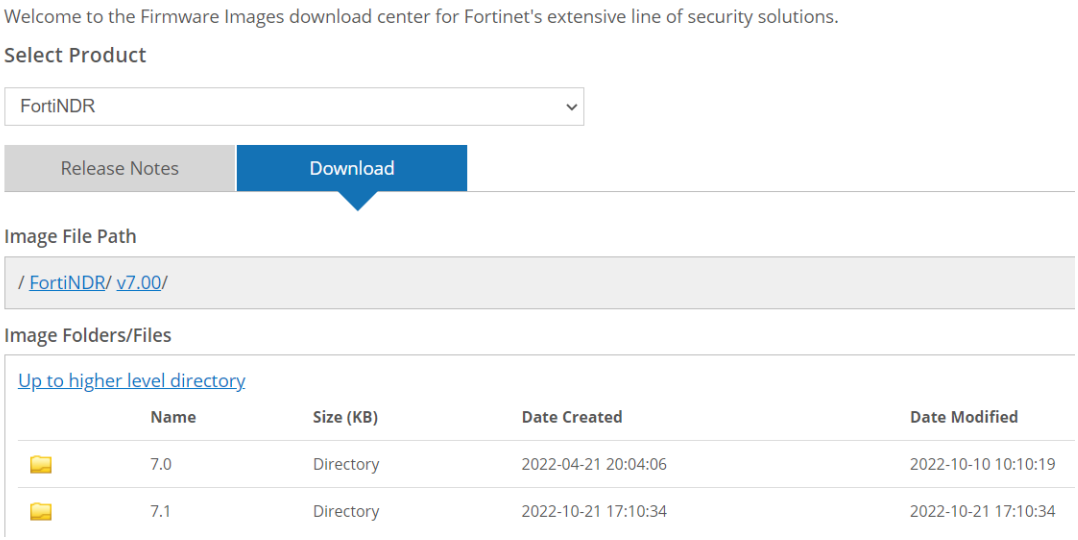
# Downloading the latest firmware version

**To download the latest version of FortiNDR:**

1. Log into FortiCloud.
2. In the banner, click *Support* > *Firmware Download*.




3. From the *Select Product* dropdown, select *FortiNDR*.
4. Click the *Download* tab.
5. Use the folders in the directory to locate and download the latest firmware version.




# Upgrading the firmware version

**Before you begin:**

You should always backup your system configuration before upgrading the firmware on your device.

Be aware the following settings are not backed up to the configuration file:

- *Network Share*
- *Network Share Quarantine*
- *File size limit*
- *Email Alert Recipients*

Record these settings so you can manually restore them after upgrade.

The *File size limit* can be found by pressing the Tab key in the following CLI:

```
execute file-size-threshold {ICAP|OFTP|inline-blocking|manual-upload|network-share|sniffer}
<size_limit_1-10240MB>
```

```
FortiNDR-VM # exec file-size-threshold ICAP
<Size Limit>           A integer between 1~10240 for size in MB

  --- current value ---
ICAP:  200 MB
```

Please make a note for each file input value.

These settings cannot be recovered after they are removed.

**To upgrade the FortiNDR firmware version:**

1. Back up the configuration file:
   a. Click the Account menu at the top-right of the page.
   b. Go to *Configuration* > *Backup*. The configuration file is saved to your computer.
2. Upgrade the firmware:
   a. Go to *System* > *Firmware*.
   b. Click *Upload* and navigate to the location of the file you downloaded from FortiCloud.
   c. Click *OK*. After the firmware is upgraded the system reboots.
   d. After the upgrade is complete, the new version of firmware should be ready. In the case where the firmware upgrade does not follow the upgrade path. or there is a VM hosting hardware failure, or a power outage during upgrade, please consider to use following CLI to restore the database.

      ```
      execute db restore
      ```

      This command will format the database and remove all the logs and the following settings: *Device input*, *Network Share*, *Network Share Quarantine*, *File size limit* and *Email Alert Recipients*.
3. Use the configuration settings you recorded earlier to manually restore the settings. For *Device Input*, you just need to re-authorize the device again.

# FortiNDR version 7.4.8

This document provides information about FortiNDR version 7.4.8 build 0545.

These Release Notes include the following topics:



## New features and enhancements

FortiNDR 7.4.8includes performance improvements but does not introduce any new features or enhancements.

## System integration and support

The following integration is tested and supported in FortiNDR 7.4.8.

| | |
|---|---|
| **FOS/FortiGate** | • FortiNDR Fabric Device widgets including *Detection Statistics* and *System Information* supported in FOS 7.0.5 and higher, and 7.2.4 and higher<br>• File submission: FOS 6.4.0 and higher<br>(FOS 6.2 and 6.4 file submission with OFTP, via the FortiSandbox field, is tested and compatible)<br>• FortiGate inline blocking (with AV profile) is supported in FOS 7.0.1 and higher (via HTTP2).<br>• FortiGate quarantine via webhook 6.4.0 and higher. |
| **FortiProxy** | • HTTP2 file submission from FortiProxy 7.0.0 and higher<br>• FortiProxy inline blocking (with AV profile) is supported in FPX 7.0.0 and higher. |
| **FortiAnalyzer** | • FortiAnalyzer integration is supported in FortiAnalyzer 7.0.1 and higher. |
| **FortiSIEM** | • Integration is supported in version 6.3.0 and higher. |
| **FortiSandbox** | • FortiSandbox integration (API submission from FortiSandbox to FortiNDR) is supported from FortiSandbox version 4.0.1 and higher. |
| **FortiMail** | • Version 7.2.0 |

| | |
|---|---|
| **FortiAuthenticator** | • FortiAuthenticator v6.4.5 and higher is supported for 2FA token login with the GUI. Push tokens are not supported at this time. |
| **ICAP** | • FortiGate 6.4.0 and higher.<br>• FortiWeb 6.3.11 and higher.<br>• Squid and other compatible ICAP clients.<br>• FortiProxy 7.0.0.<br>• FortiNAC quarantine support (v9.2.2+)<br>• FortiAuthenticator v6.4.5 and higher is supported for 2FA token login with the GUI. Push tokens are not supported at this time.<br>• FortiSwitch quarantine via FortiLink (FortiSwitch v7.0.0+ and FortiGate v7.0.5+)<br>  FortiNDR 7.0.1 and later supports sending both malware and NDR logs to FortiAnalyzer and FortiSIEM or other syslog devices.<br>FortiAnalyzer 7.2.0 supports receiving logs from FortiNDR (log view only).<br>FortiAnalyzer 7.2.1 supports reporting based on logs. |

# Supported models

FortiNDR version 7.4.8 supports the following models:

| Model | Mode | Details |
|---|---|---|
| FortiNDR-1000F | Standalone and Sensor | |
| FortiNDR-3500F gen3* | Standalone and Center | Supports FortiNDR central management.<br>For hardware details please visit hardware quick start guide or the following notice. |
| FortiNDR VM | Standalone, Sensor and Center | |
| FortiNDR KVM | Standalone, Sensor and Center | |
| FortiNDR on AWS (BYOL) | Standalone, Sensor and Center | |
| FortiNDR on GCP (BYOL) | Standalone, Sensor and Center | |
| FortiNDR on Alibaba (BYOL) | Standalone | |
| FortiNDR on Azure (BYOL) | Standalone, Sensor and Center | |

## *Notice about hardware generations

The hardware model is printed on the label on the back of the unit.

- FortiNDR gen3 - P24935-03 supports v7.1.x, v7.2.x, and 7.4.x
- FortiAI gen1 - P24935-01 does not support 7.1.x and 7.2.x
- FortiAI gen2 - P24935-02 does not support 7.1.x and 7.2.x

**To confirm the hardware generation with the CLI:**

```
get system status
```

This allows you to check the BIOS version. Gen3 models use BIOS version *00010031* and above. Any version below *00010031*, such as *00010001*, indicates a Gen2 or Gen1 model.

# Resolved issues

The following issues have been fixed in version 7.4.8. For inquires about a particular bug, contact Customer Service & Support.

## Common Vulnerabilities and Exposures

| Bug ID | Description |
|---|---|
| 1147099 | FortiNDR 7.4.8 is no longer vulnerable to the following CVE Reference:<br>• CVE-2025-32756 |

# Known issues

The following issues have been identified in version 7.4.8. For inquires about a particular bug or to report a bug, contact Customer Service & Support.

| Bug ID | Description |
|---|---|
| 1151818 | FortiNDR may stop logging events when it detects a high volume of anomalies |

www.fortinet.com